



**Application Notes for Configuring ATT-AudioText Telecom
AG Alarm Management Server with Avaya Aura®
Communication Manager R6.3 and Avaya Aura® Session
Manager R6.3 – Issue 1.0**

Abstract

These Application Notes describe the configuration steps for provisioning ATT-AudioText Telecom AG Alarm Management Server to interoperate with Avaya Aura® Communication Manager and Avaya Aura® Session Manager.

Information in these Application Notes has been obtained through DevConnect compliance testing and additional technical discussions. Testing was conducted via the DevConnect Program at the Avaya Solution and Interoperability Test Lab.

1. Introduction

These Application Notes describe the configuration steps required for ATT-AudioText Telecom AG Alarm Management Server to successfully interoperate with Avaya Aura® Communication Manager R6.3 and Avaya Aura® Session Manager R6.3. The ATT-AudioText Telecom AG Alarm Management Server (ATT AMX) generates preconfigured or ad hoc alarms which were signaled to Communication Manager as calls via a SIP Trunk between the ATT-AudioText Telecom AG Alarm Management Server and Avaya Aura® Session Manager.

2. General Test Approach and Test Results

The interoperability compliance testing evaluates the ability of The ATT AMX server to send an Alarm notification both aurally and visually to various Avaya endpoints. For the conformance tests described by these Application Notes, ATT AMX Alarm Management Server and Communication Manager were configured to operate as follows:

- Each alarm consisted of an audio message and a text message. The text message was sent as the calling party name (which can have a maximum length of fifteen characters) and was thus visible for alarms to local extensions and DECT endpoints (but not PSTN endpoints).
- Alarms were also configured such that the alarm recipient must acknowledge via keypad input, thus preventing alarms which were answered by voicemail systems from being considered as delivered.

DevConnect Compliance Testing is conducted jointly by Avaya and DevConnect members. The jointly-defined test plan focuses on exercising APIs and/or standards-based interfaces pertinent to the interoperability of the tested products and their functionalities. DevConnect Compliance Testing is not intended to substitute full product performance or feature testing performed by DevConnect members, nor is it to be construed as an endorsement by Avaya of the suitability or completeness of a DevConnect member's solution.

2.1. Interoperability Compliance Testing

The compliance testing included the test scenarios shown below. Note that when applicable, all tests were performed with Avaya SIP deskphones, Avaya H.323 deskphones, Avaya DECT handsets and PSTN endpoints.

- Alarm creation via text-to-speech and via telephone input
- Alarm delivery to idle station
- Alarm to busy station
- Alarm to station, no answer
- Alarm to station with coverage enabled, no answer
- Alarm to station with call forwarding enabled
- Alarm to unavailable station
- Alarm to tandem station
- Alarm to hunt group
- Alarm to multiple endpoints
- Automatic startup after power interruption
- Recovery from interruption to interface to PBX

2.2. Test Results

The following observations were noted during testing.

- If a local fixed extension which has no available call appearance receives an incoming alarm call, the caller receives a “busy” indication: it makes no difference if it is a “priority” call.
- If an alarm call is made to a diverted (call forwarding) station, the call is diverted: it makes no difference if it is a “priority” call.
- Alarm calls to fixed stations which are paired with DECT stations via EC500, result in calls to DECT stations which do not include alarm text messages.
- If the ATT AMX Alarm Management Server is disconnected from its LAN interface, no alarms will be generated. The unit continues normal operation when the LAN interface is reconnected.

2.3. Support

Support from Avaya is available by visiting the website <http://support.avaya.com> and a list of product documentation can be found in **Section 10** of these Application Notes. Product information and support for ATT AG products may be found at:

- Website: www.attag.ch/en/contact-us
- Help desk: +41 (0)44 908 60 04

3. Reference Configuration

Figure 1 shows the network topology during compliance testing. The ATT AMX server is connected to the telephony LAN and registers with Session Manager in order to be able to send alarms to the Avaya H.323 and SIP deskphones on Communication Manager.

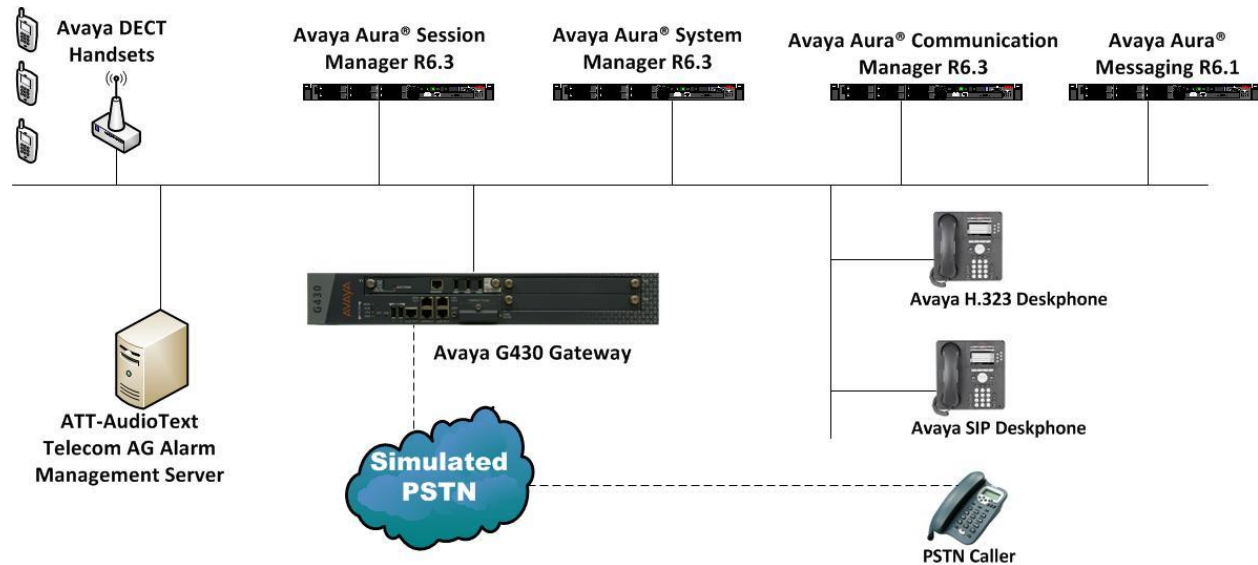


Figure 1: Network Solution of ATT-AudioText Telecom AG Alarm Management Server with Avaya Aura® Communication Manager R6.3 and Avaya Aura® Session Manager R6.3

4. Equipment and Software Validated

The following equipment and software was used for the compliance test.

Equipment/Software	Version/Release
Avaya Aura [®] System Manager running on an Avaya S8800 Server	R6.3 SP3 Build 6.3.0.8.5682-6.3.8.1814 Software Update Revision 6.3.3.5.1719
Avaya Aura [®] Communication Manager running on an Avaya S8800 Server	R6.3 SP1 R016x.03.0.124.0
Avaya Aura [®] Session Manager running on an Avaya S8800 Server	R6.3 SP3 6.3.3.0.633004
Avaya 9608 H.323 Deskphone Avaya 9620 H.323 Deskphone Avaya 9630 SIP Deskphone	96xx H.323 Release 6.2009 96xx H.323 Release 3.103 (SP2) 96xx SIP Release 2.6.8.4 (SP3)
Avaya 9621 H.323 Deskphone Avaya 9641 H.323 Deskphone Avaya 9641 SIP Deskphone	96x1 H.323 Release 6.2.119 96x1 H.323 Release 6.2209 96x1 SIP Release 6.2.1.26
Avaya one-X [®] Communicator	R6.1
Avaya DECT Handsets	3725 DH4 (R3.3.11) 3720 DH3 (R3.3.11)
ATT-AudioText Telecom AG Alarm Management Server	V11.4.8.52

5. Configure Avaya Aura® Communication Manager

It is assumed that a fully functioning Communication Manager is in place with the necessary licensing with a SIP Trunk in place to Session Manager. For further information on the configuration of Communication Manager please see **Section 10** of these Application Notes. The following sections go through the following.

- Dial Plan Analysis
- IP Interfaces
- Network Region
- IP Codec
- SIP Trunk

5.1. Configure Dial Plan Analysis

Use the **change dialplan analysis** command to configure the dial plan using the parameters shown below. Extension numbers (**ext**) are those beginning with **2, 3, 4** and **5**. Feature Access Codes (**fac**) use digits **8** and **9** or **#**.

change dialplan analysis									Page 1 of 12	
DIAL PLAN ANALYSIS TABLE										
Location: all									Percent Full: 1	
Dialed String	Total Length	Call Type	Dialed String	Total Length	Call Type	Dialed String	Total Length	Call Type		
2	4	ext								
3	4	ext								
4	4	ext								
5	4	ext								
8	1	fac								
9	1	fac								
*	3	dac								
#	3	fac								

5.2. Configure IP Interfaces

Shown below is an example of the nodes names used in the compliance testing. Note that ATT AMX does not feature in this setup and only the name and IP address of Session Manager is added. Use the **change node-names ip** command to configure the IP address of Session Manager. **SM100** is the **Name** used for Session Manager and **10.10.40.34** is the **IP Address**.

change node-names ip		IP NODE NAMES		Page 1 of 2	
Name	IP Address				
SM100	10.10.40.34				
default	0.0.0.0				
G430	10.10.40.18				
procr	10.10.40.13				
procr6	::				

5.3. Configure Network Region

Use the **change ip-network-region x** (where x is the network region to be configured) command to assign an appropriate domain name to be used by Communication Manager, in the example below **devconnect.local** is used. Note this domain is also configured in **Section 6.1** of these Application Notes.

```
change ip-network-region 1                                     Page 1 of 20

                                IP NETWORK REGION

Region: 1
Location: 1      Authoritative Domain: devconnect.local
Name: default NR
MEDIA PARAMETERS                      Intra-region IP-IP Direct Audio: yes
Codec Set: 1      Inter-region IP-IP Direct Audio: yes
UDP Port Min: 2048                                IP Audio Hairpinning? y
UDP Port Max: 3329
DIFFSERV/TOS PARAMETERS
Call Control PHB Value: 46
Audio PHB Value: 46
Video PHB Value: 26
802.1P/Q PARAMETERS
Call Control 802.1p Priority: 6
Audio 802.1p Priority: 6
Video 802.1p Priority: 5      AUDIO RESOURCE RESERVATION PARAMETERS
H.323 IP ENDPOINTS                      RSVP Enabled? n
H.323 Link Bounce Recovery? y
Idle Traffic Interval (sec): 20
Keep-Alive Interval (sec): 5
Keep-Alive Count: 5
```

5.4. Configure IP-Codec-Set

Use the **change ip-codec-set x** (where x is the ip-codec set used) command to designate a codec set compatible with the ATT AMX which supports both **G.711A** and **G.729A**.

```
change change ip-codec-set 1                                     Page 1 of 2

                                IP Codec Set

Codec Set: 1

Audio      Silence      Frames      Packet
Codec      Suppression   Per Pkt    Size(ms)
1: G.711A      n           2          20
2: G.729A      n           2          20
```

5.5. Configure SIP Trunk

Prior to configuring a SIP trunk group for communication with Session Manager, a SIP signaling group must be configured. Configure the Signaling Group form shown below as follows:

- Set the **Group Type** field to **sip**
- Set the **Transport Method** to the desired transport method; **tcp** (transport control protocol) or **tls** (Transport Layer Security)
- The **Peer Detection Enabled** field should be set to **y** allowing the Communication Manager to automatically detect if the peer server is a Session Manager
- Specify the node names for procr and the Session Manager node name as the two ends of the signaling group in the **Near-end Node Name** field and the **Far-end Node Name** field, respectively. These values are taken from the **IP Node Names** form shown above
- Set the **Near-end Node Name** to **procr**. This value is taken from the **IP Node Names** form shown above
- Set the **Far-end Node Name** to the node name defined for the Session Manager (node name **SM100**), also shown above
- Ensure that the recommended TLS port value of **5061** is configured in the **Near-end Listen Port** and the **Far-end Listen Port** fields
- In the **Far-end Network Region** field, enter the IP Network Region configured above. This field logically establishes the **far-end** for calls using this signaling group as network region 1
- Leave the **Far-end Domain** field blank to allow Communication Manager to accept any domain
- The **DTMF over IP** field should remain set to the default value of **rtp-payload**. This value enables Communication Manager to send DTMF transmissions using RFC 2833
- The **Direct IP-IP Audio Connections** field is set to **y**
- The default values for the other fields may be used

change signaling-group 1		Page 1 of 2
SIGNALING GROUP		
Group Number: 1	Group Type: sip	
IMS Enabled? n	Transport Method: tls	
Q-SIP? n		
IP Video? n		Enforce SIPS URI for SRTP? y
Peer Detection Enabled? y	Peer Server: SM	
Near-end Node Name: procr	Far-end Node Name: SM100	
Near-end Listen Port: 5061	Far-end Listen Port: 5061	
	Far-end Network Region: 1	
Far-end Domain:		
Incoming Dialog Loopbacks: eliminate	Bypass If IP Threshold Exceeded? n	
DTMF over IP: rtp-payload	RFC 3389 Comfort Noise? n	
Session Establishment Timer(min): 3	Direct IP-IP Audio Connections? y	
Enable Layer 3 Test? y	IP Audio Hairpinning? n	
H.323 Station Outgoing Direct Media? n	Initial IP-IP Direct Media? n	
	Alternate Route Timer(sec): 6	

Configure the **Trunk Group** form as shown below. This trunk group is used for alarm calls from the ATT AMX Server. Enter a descriptive name in the **Group Name** field. Set the **Group Type** field to **sip**. Enter a **TAC** code compatible with the Communication Manager dial plan. Set the **Service Type** field to **tie**. Specify the signaling group associated with this trunk group in the **Signaling Group** field, and specify the **Number of Members** supported by this SIP trunk group. Accept the default values for the remaining fields.

```

change trunk-group 1                                     Page 1 of 21
                                TRUNK GROUP

Group Number: 1                      Group Type: sip          CDR Reports: y
  Group Name: SIP TRK                COR: 1                TN: 1          TAC: *11
    Direction: two-way              Outgoing Display? y
    Dial Access? n
    Queue Length: 0
  Service Type: tie                  Auth Code? n
                                      Member Assignment Method: auto
                                      Signaling Group: 1
                                      Number of Members: 10

```

On **Page 2** of the trunk-group form the **Preferred Minimum Session Refresh Interval (sec)** field should be set to a value mutually agreed with the ATT AMX Server to prevent unnecessary SIP messages during call setup. For the compliance test a value of **600** was used.

```

change trunk-group 1                                     Page 2 of 21
  Group Type: sip

TRUNK PARAMETERS

  Unicode Name: auto

                                      Redirect On OPTIM Failure: 5000

    SCCAN? n                          Digital Loss Group: 18
      Preferred Minimum Session Refresh Interval(sec): 600

  Disconnect Supervision - In? y  Out? y

                                      XOIP Treatment: auto    Delay Call Setup When Accessed Via IGAR? N

```

Settings on **Page 3** can be left as default.

change trunk-group 1	Page 3 of 21
TRUNK FEATURES	
ACA Assignment? n	Measured: none
	Maintenance Tests? y
Numbering Format: private	UI Treatment: service-provider
	Replace Restricted Numbers? n
	Replace Unavailable Numbers? n
Modify Tandem Calling Number: no	
Show ANSWERED BY on Display? y	

Settings on **Page 4** are as follows.

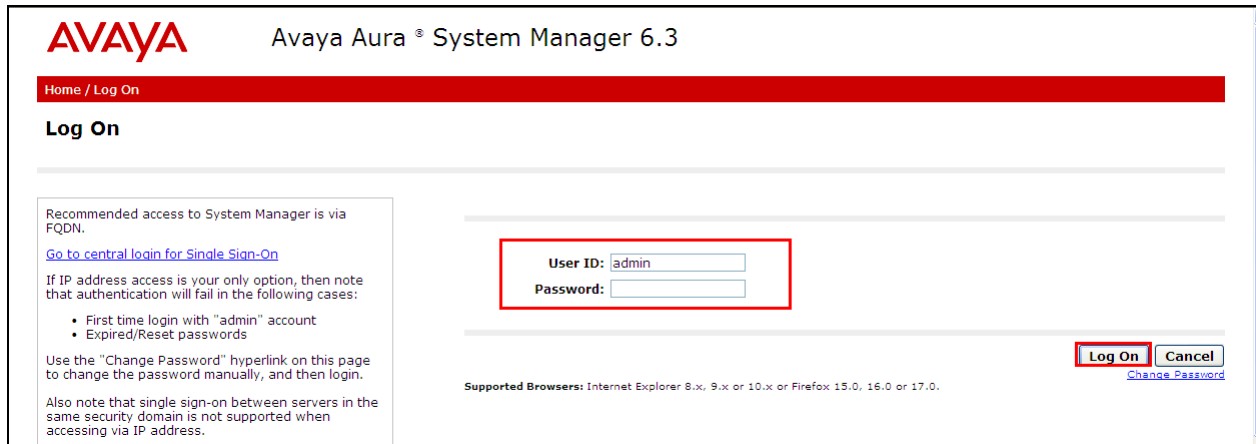
change trunk-group 1	Page 4 of 21
PROTOCOL VARIATIONS	
Mark Users as Phone? n	
Prepend '+' to Calling/Alerting/Diverting/Connected Number? n	
Send Transferring Party Information? y	
Network Call Redirection? n	
Send Diversion Header? n	
Support Request History? y	
Telephone Event Payload Type: 101	
Convert 180 to 183 for Early Media? n	
Always Use re-INVITE for Display Updates? n	
Identity for Calling Party Display: P-Asserted-Identity	
Block Sending Calling Party Location in INVITE? n	
Accept Redirect to Blank User Destination? y	
Enable Q-SIP? n	

6. Configure Avaya Aura® Session Manager

A SIP trunk is setup between the ATT AMX server and Session Manager. In order to make changes in Session Manager a web session to System Manager is opened.

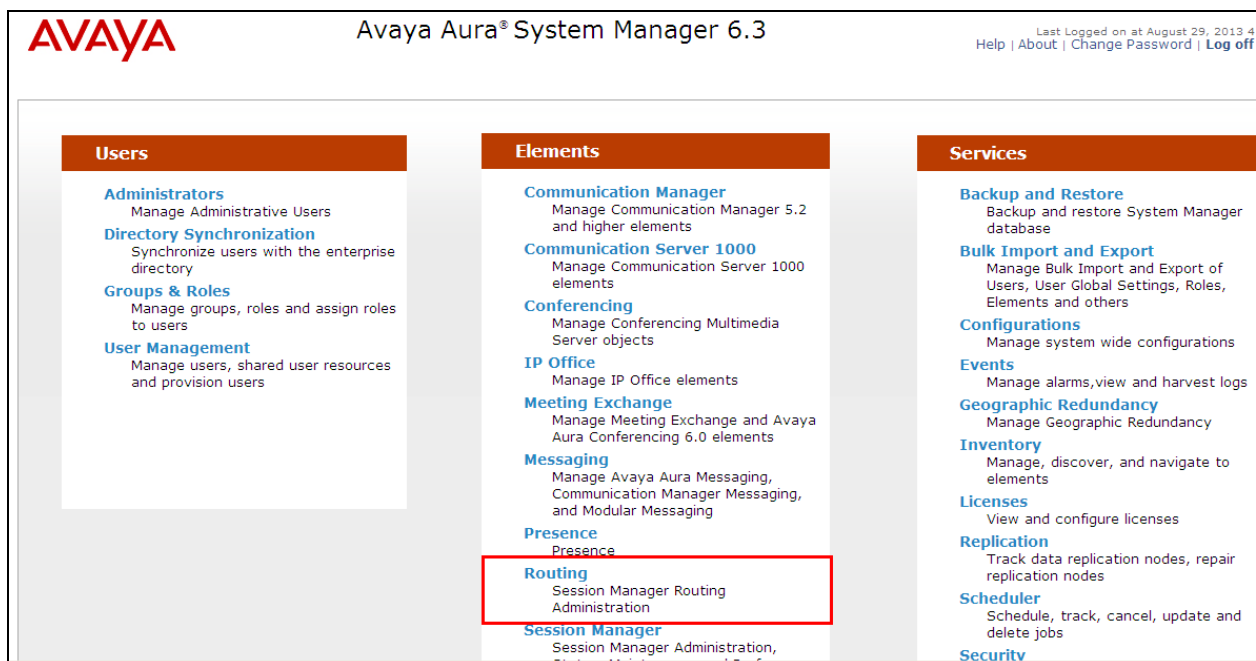
6.1. Configuration of a Domain

Navigate to <http://<System Manager IP Address>/SMGR>, enter the appropriate credentials and click on **Log On** as shown below.



The screenshot shows the Avaya Aura System Manager 6.3 login page. At the top, the Avaya logo and "Avaya Aura® System Manager 6.3" are displayed. Below this is a red navigation bar with "Home / Log On". The main heading is "Log On". On the left, there is a text box with instructions: "Recommended access to System Manager is via FQDN. Go to central login for Single Sign-On. If IP address access is your only option, then note that authentication will fail in the following cases: • First time login with 'admin' account • Expired/Reset passwords. Use the 'Change Password' hyperlink on this page to change the password manually, and then login. Also note that single sign-on between servers in the same security domain is not supported when accessing via IP address." In the center, there is a login form with "User ID: admin" and a blank "Password:" field. To the right of the form are "Log On" and "Cancel" buttons, and a "Change Password" link. At the bottom, it lists "Supported Browsers: Internet Explorer 8.x, 9.x or 10.x or Firefox 15.0, 16.0 or 17.0."

Once logged in click on **Routing** highlighted below.



The screenshot shows the main menu of Avaya Aura System Manager 6.3 after logging in. The top bar includes the Avaya logo, "Avaya Aura® System Manager 6.3", and a "Last Logged on at August 29, 2013 4" timestamp with links for "Help", "About", "Change Password", and "Log off". The main content area is divided into three columns: "Users", "Elements", and "Services". Under "Users", there are links for "Administrators", "Directory Synchronization", "Groups & Roles", and "User Management". Under "Elements", there are links for "Communication Manager", "Communication Server 1000", "Conferencing", "IP Office", "Meeting Exchange", "Messaging", "Presence", "Routing" (highlighted with a red box), and "Session Manager". Under "Services", there are links for "Backup and Restore", "Bulk Import and Export", "Configurations", "Events", "Geographic Redundancy", "Inventory", "Licenses", "Replication", "Scheduler", and "Security".

Click on **Domains** in the left window. If there is not a domain already configured, click on **New** highlighted below.

The screenshot shows the Avaya Aura System Manager 6.3 interface. On the left, the 'Routing' menu is expanded, and 'Domains' is highlighted with a red box. The main area is titled 'Domain Management' and shows a table with 2 items. The 'New' button is highlighted with a red box.

Name	Type	Notes

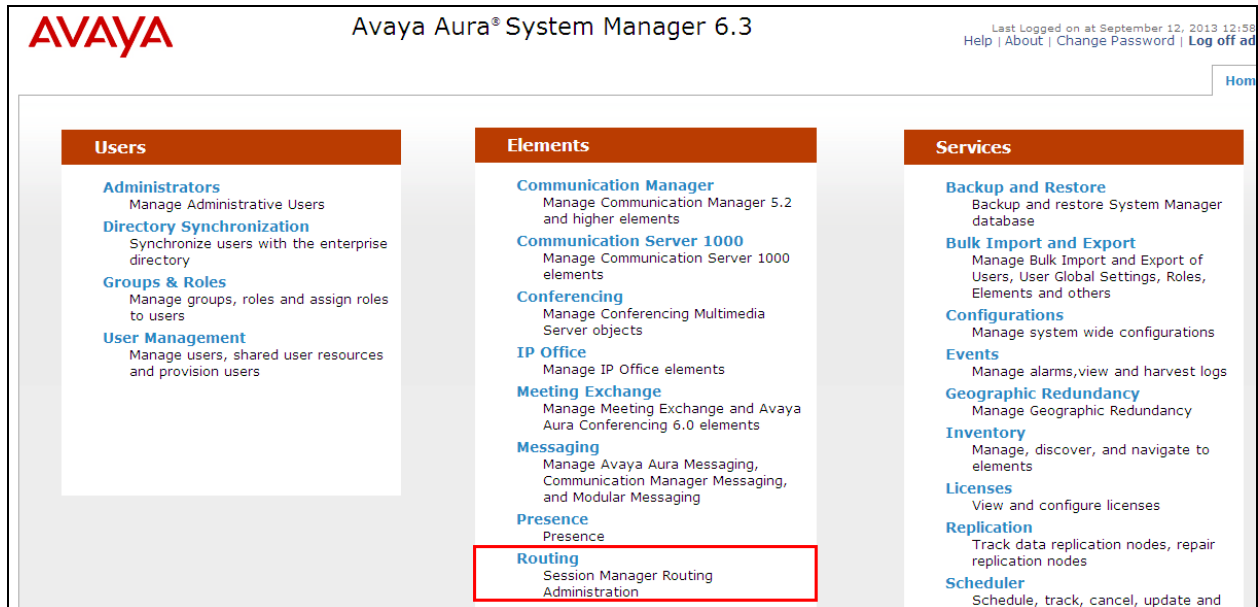
Note the domain **Name** used in the compliance testing was **devconnect.local**. Note this domain is also referenced in **Section 5.3**. Once the domain name is entered click on **Commit** to save this.

The screenshot shows the Avaya Aura System Manager 6.3 interface. On the left, the 'Routing' menu is expanded, and 'Domains' is highlighted with a red box. The main area is titled 'Domain Management' and shows a table with 1 item. The 'Commit' button is highlighted with a red box.

Name	Type	Notes
devconnect.local	sip	

6.2. Configuration of SIP Entities

Navigate to <http://<System Manager IP Address>/SMGR>, enter the appropriate credentials and click on **Log On** as shown in **Section 6.1**. Once logged in, click on **Routing** highlighted below.



Clicking on **SIP Entities** shows what SIP Entities have been added to the system and allows the addition of any new SIP Entity that may be required. Please note the SIP Entities already present for the Compliance Testing of ATTAG AMX Server.

- Communication Manager SIP Entity
- Session Manager SIP Entity

A SIP Entity and Entity link are required in order for the Alarm server to send the alarm message to Communication Manager Stations. Select **SIP Entities** in the left window and click on **New** in the main window.

The screenshot shows the Avaya Aura System Manager 6.3 interface. On the left, the 'Routing' menu is expanded, and 'SIP Entities' is highlighted. The main window displays the 'SIP Entities' page with a 'New' button highlighted in a red box. Below the buttons is a table with 8 items. The table has columns for Name, FQDN or IP Address, Type, and Notes.

Name	FQDN or IP Address	Type	Notes
AAMessaging	192.168.50.60	SIP Trunk	
ASCOMDECT1	10.10.40.181	SIP Trunk	
CM62	192.168.50.13	CM	
CM63VMPPG	10.10.40.31	CM	
CS1KPG1	10.10.40.111	SIP Trunk	
CS1KPG2	192.168.50.99	SIP Trunk	

Enter a suitable **Name** and enter the **IP Address** of the ATT AMX Server. Select the correct **Location** and **Time Zone**. Click on **Commit** once completed.

The screenshot shows the 'SIP Entity Details' page in Avaya Aura System Manager 6.3. The 'General' tab is selected. The 'Name' field is set to 'ATTAG', the 'FQDN or IP Address' field is set to '10.10.40.80', and the 'Type' is set to 'SIP Trunk'. The 'Location' is set to 'DevConnectPG63' and the 'Time Zone' is set to 'Europe/Dublin'. The 'Commit' button is highlighted in a red box.

Select **Entity Links** from the left window and select **New** from the right window in order to add the new ATT AMX Entity Link.

Avaya Aura® System Manager 6.3

Home / Elements / Routing / Entity Links

Entity Links

[New](#) [Edit](#) [Delete](#) [Duplicate](#) [More Actions](#)

7 Items Refresh

<input type="checkbox"/>	Name	SIP Entity 1	Protocol	Port	SIP Entity 2	Port	Connection Policy	Deny New Service
<input type="checkbox"/>	AAMessaging	SM63vmppg	TCP	5060	AAMessaging	5060	trusted	<input type="checkbox"/>
<input type="checkbox"/>	ASCOMDECT1	SM63vmppg	TCP	5060	ASCOMDECT1	5060	trusted	<input type="checkbox"/>
<input type="checkbox"/>	SM63vmppg_CM62_5061_TLS	SM63vmppg	TLS	5061	CM62	5061	trusted	<input type="checkbox"/>
<input type="checkbox"/>	SM63vmppg_CM63VMPPG_5061_TLS	SM63vmppg	TLS	5061	CM63VMPPG	5061	trusted	<input type="checkbox"/>
<input type="checkbox"/>	SM63vmppg_CS1KPG1_5060_TCP	SM63vmppg	TCP	5060	CS1KPG1	5060	trusted	<input type="checkbox"/>
<input type="checkbox"/>	SM63vmppg_CS1KPG2_5060_TCP	SM63vmppg	TCP	5060	CS1KPG2	5060	trusted	<input type="checkbox"/>
<input type="checkbox"/>	SM63vmppg_NRS76_5060_TCP	SM63vmppg	TCP	5060	NRS76	5060	trusted	<input type="checkbox"/>

Select : All, None

Ensure that **UDP** is selected for the **Protocol** and **5060** for the **Port**. Click on **Commit** once completed.

Avaya Aura® System Manager 6.3

Home / Elements / Routing / Entity Links

Entity Links

[Commit](#) [Cancel](#)

1 Item

<input type="checkbox"/>	Name	SIP Entity 1	Protocol	Port	SIP Entity 2	DNS Override	Port	Connection Policy	Deny New Service	Notes
<input type="checkbox"/>	*ATTAG	*SM63vmppg	UDP	*5060	*ATTAG	<input type="checkbox"/>	*5060	trusted	<input type="checkbox"/>	

Select : All, None

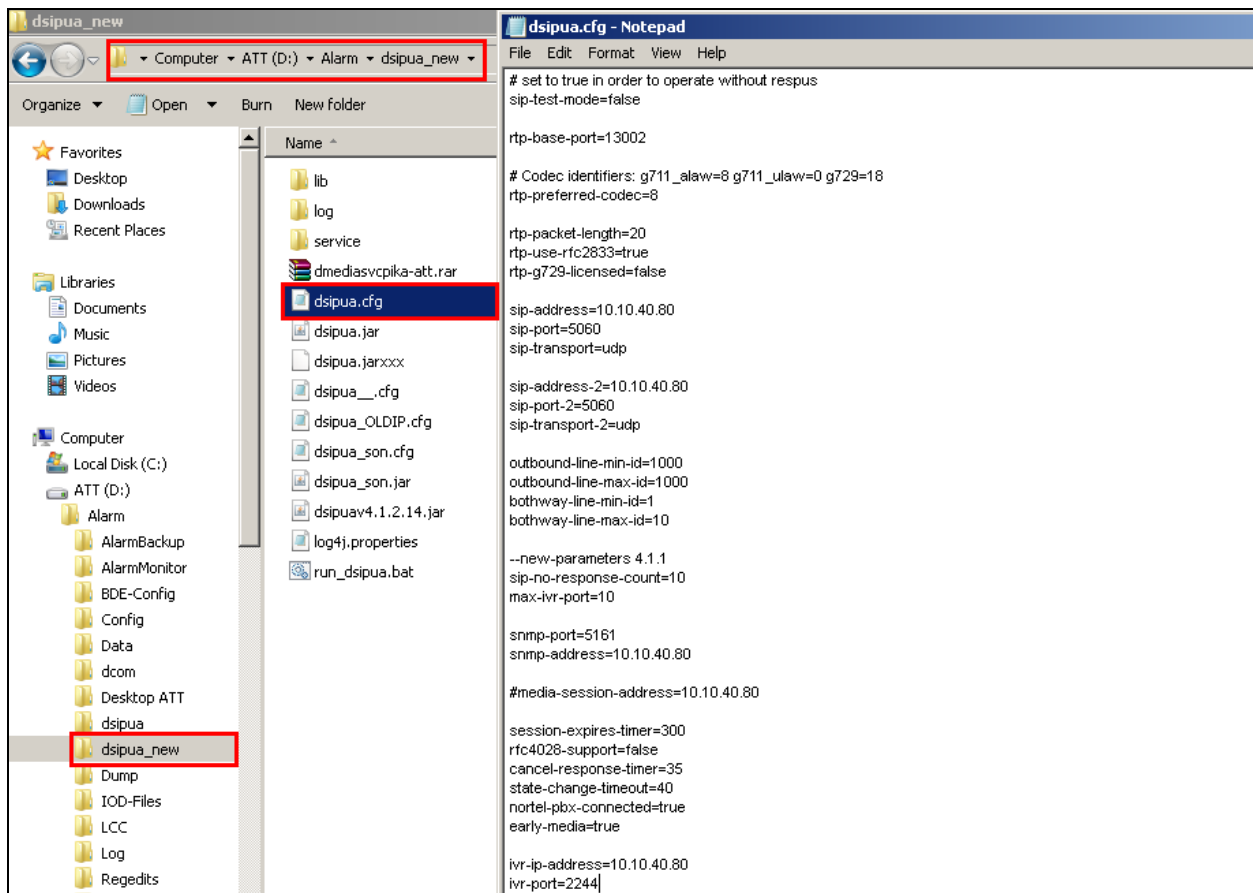
[Commit](#) [Cancel](#)

7. Configure ATT-AudioText Telecom AG Alarm Management Server

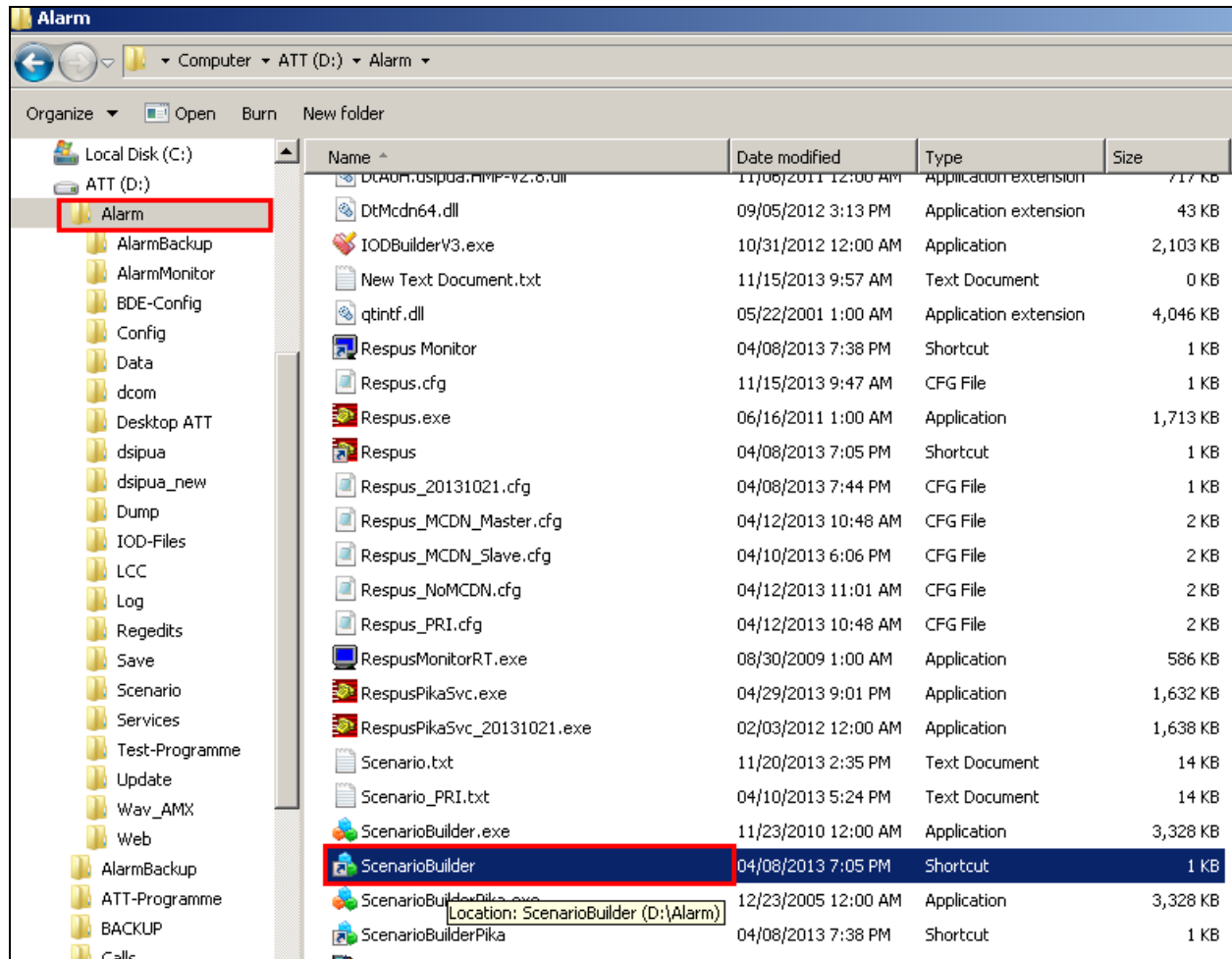
The configuration of the ATT AMX server involves the SIP connection between the AMX Alarm server and Session Manager also the addition of the extension(s) to call on Communication Manager to issue the alarm notification.

7.1. Configuring the SIP connection to Session Manager

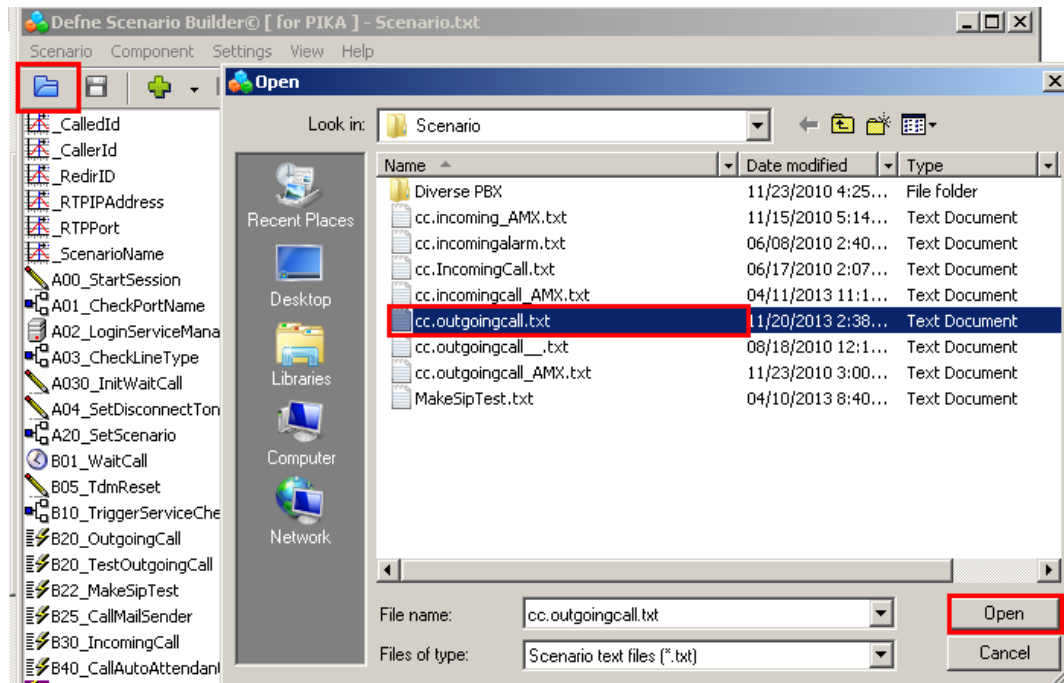
During the initial installation of AMX a folder called Alarm is created. Navigate to **Alarm→dsipua_new**, open file called **dsipua.cfg**. Note the address below **10.10.40.80** is the IP address of the AMX server. The **sip-port** used is **5060** and the **sip-transport** is **udp**. All remaining fields were left as default.



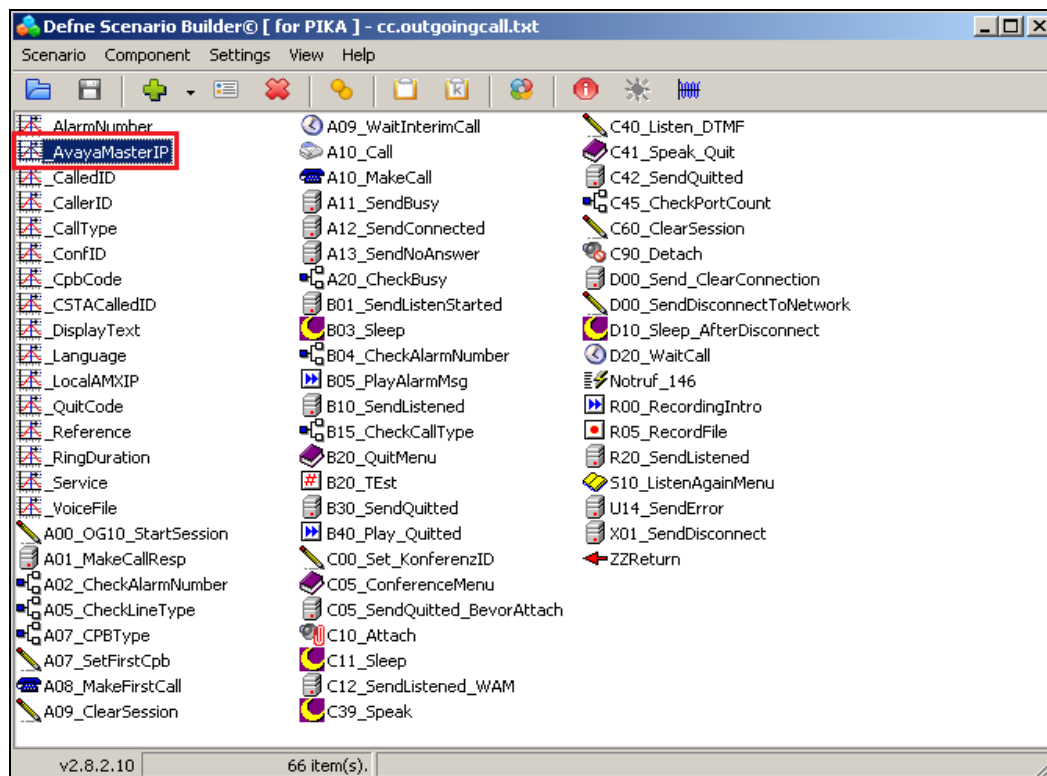
Open **ScenarioBuilder** which is also located in the **Alarm** folder.



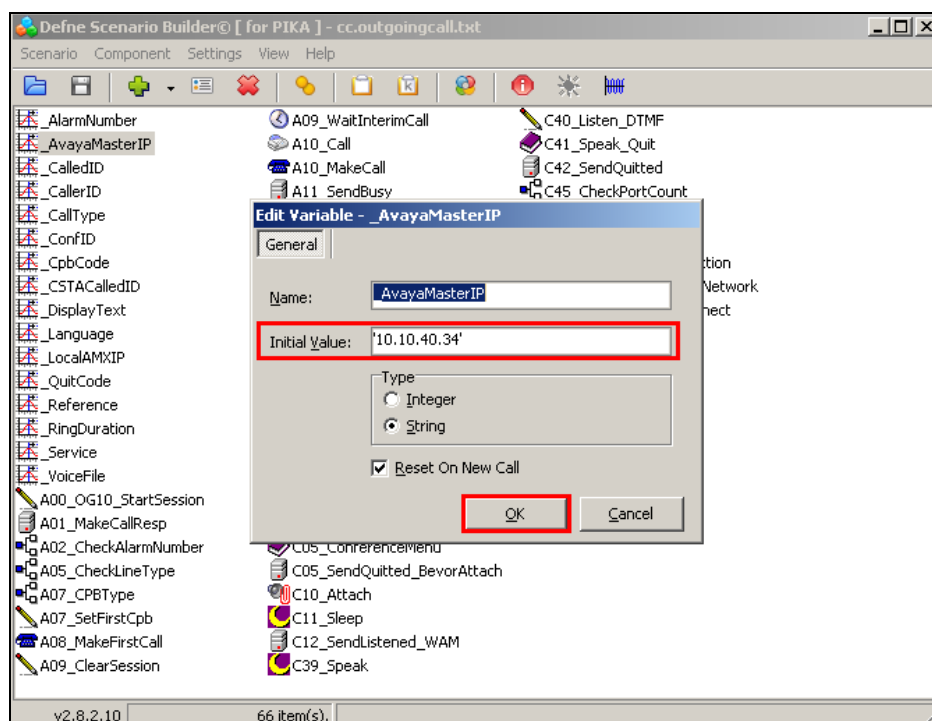
Click on the open icon at the top left of window, this opens the following window where **cc_outgoingcall.txt** is chosen and opened.



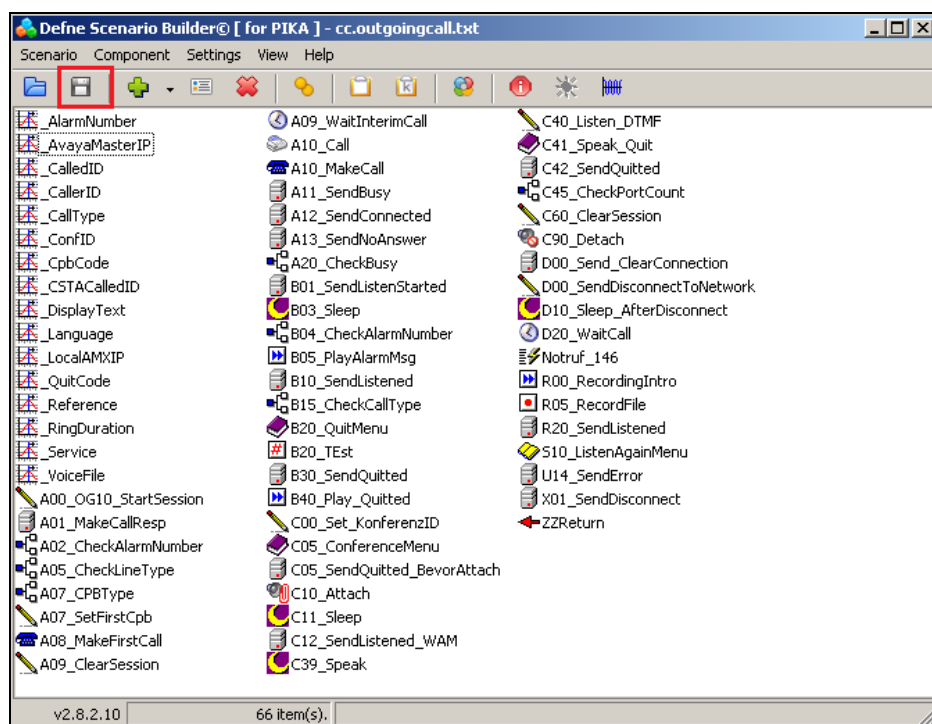
Select **_AvayaMasterIP** from the resulting window below.



Enter the IP address of the Session Manager into the **Initial Value** field. Everything else can be left as default, click on **OK** to continue.

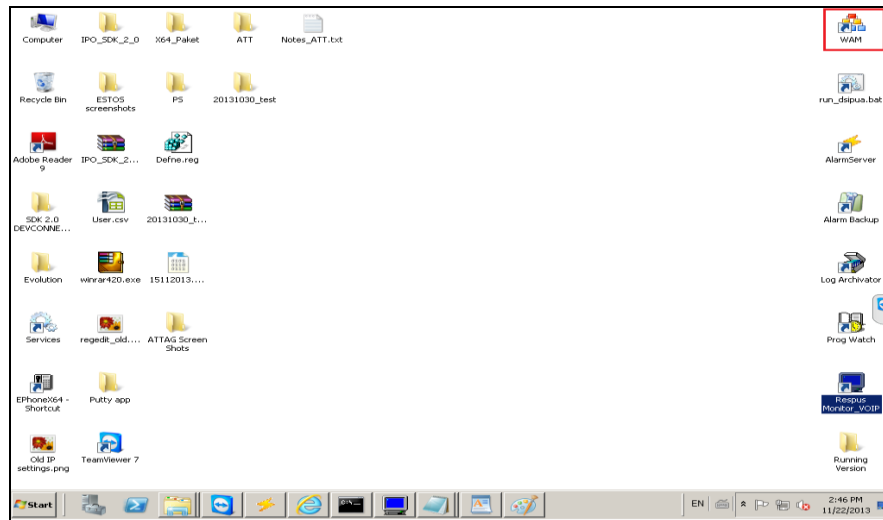


Save this file by clicking on the save icon highlighted



7.2. Adding extensions to call

This section describes the steps necessary to create the extension numbers and groups that the Alarm server will call in the event of an alarm. Open the **WAM** shortcut on the Alarm server desktop.



Enter the proper credentials for a “Super User” and click on Log in to continue.

ATT no limits in communication

Web Alarm Manager - WAM Login

Account: ATT

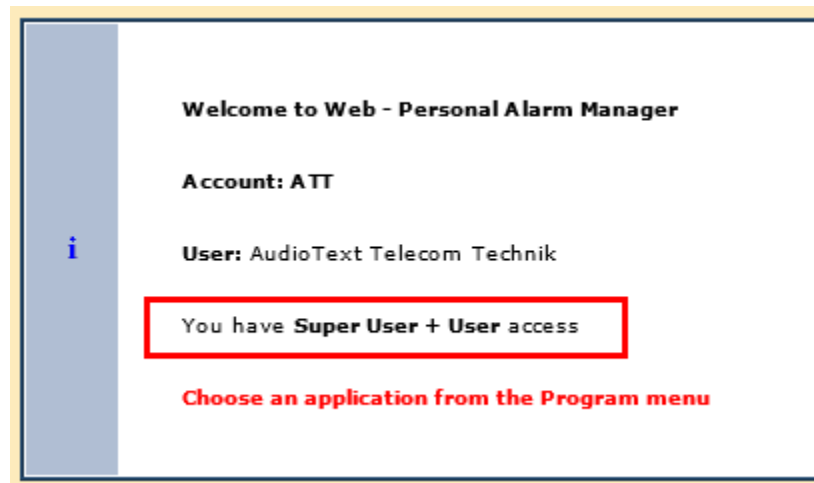
User Name:

Password:

Log in

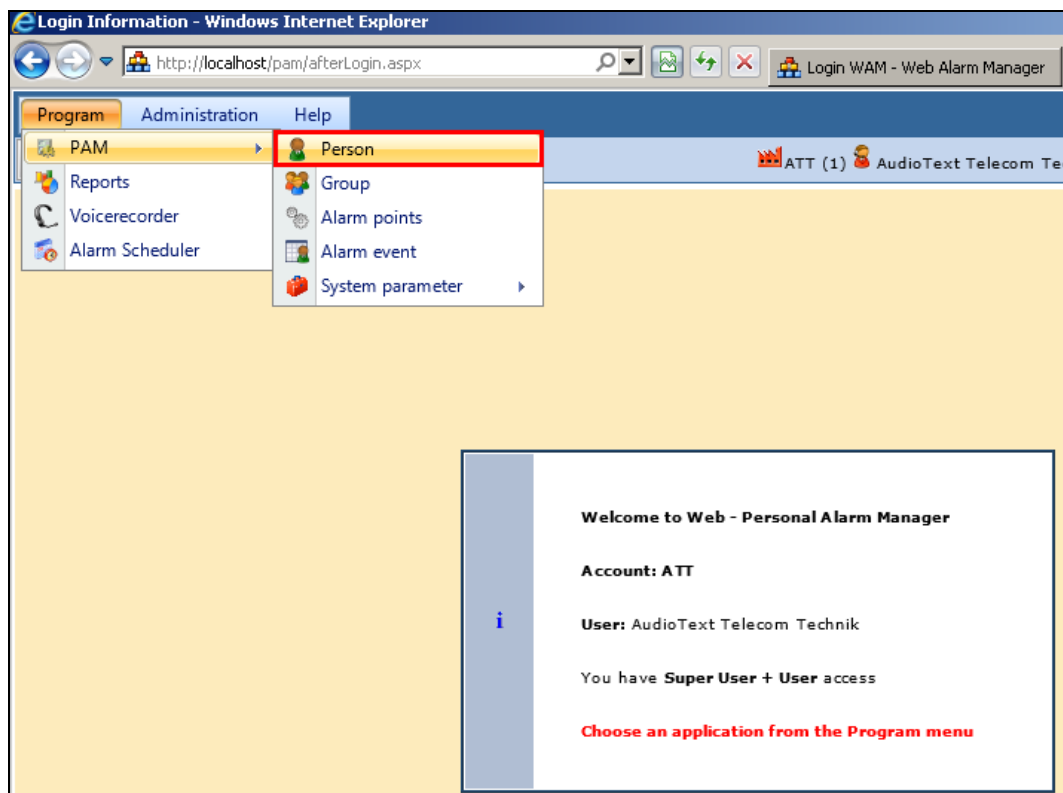
R11.4.8.52

The following screen shows that the user is logged in correctly as a Super User.



7.2.1. Add a new Person

A new extension is represented as a person in the setup. To add a new person, select **Program→PAM→Person** as shown below.



In the resulting window click on the **New** icon highlighted below.

Update Recipient

Current Recipients

Reset

+ - x

First Name	Lastname	Department	Active
	2013		Y
	2014		Y
B	2017		Y
A	3015		Y
C	3017		Y
D	3200		Y
2002	Avaya 9608 H.323 deskphone		Y
2000	Avaya 9620 H.323 deskphone		Y
2003	Avaya 9621 H.323 deskphone		Y
1001	Avaya 9630 SIP deskphone		Y

1 2 3 10 1 - 10/23

Recipient 2013 in group

Group

2013

2013*74

22252013

Enter the person or extension details as shown and ensure that **INT L-15-1** is selected as the **Notification properties** and that the extension number is entered as the **Target ID**. Then click on the **Add** icon highlighted below.

Edit recipient[2200 Avaya DECT H.323 handset - ATT]

Enhanced View

Person Remote activation

Personal data

Activated ☒

Surname Avaya DECT H.323 handset

First name 2200

E-Mail

Department

Language Default

Communication channel

Notification properties	Target ID
INT L-15-1	2200

+ - x

Save Cancel

Ensure that the **Activated** box is ticked and click **Save** once the **Target ID** has been added correctly as shown below.

Edit recipient[2200 Avaya DECT H.323 handset - ATT] Enhanced View

Person **Remote activation**

Personal data

Activated ☒

Surname Avaya DECT H.323 handset

First name 2200

E-Mail

Department

Language Default

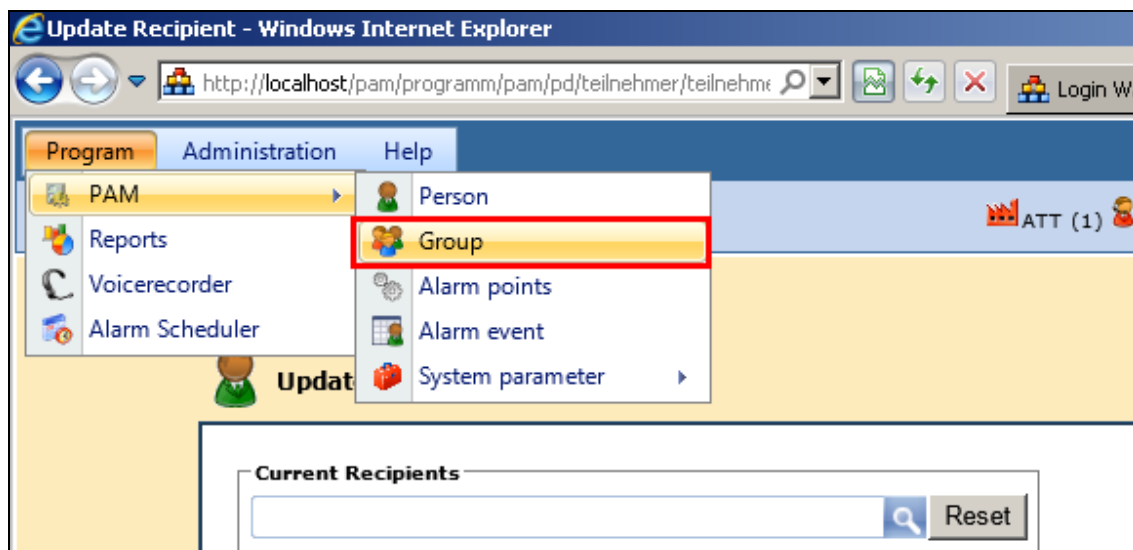
Communication channel

Notification properties	Target ID
INT L-15-1	2200
*74CFD-L-5-1	

Save **Cancel**

7.2.2. Add a new Group

A new group must be added that contains the person or people involved in this group. Select **Program**→**PAM**→**Group**.



Click on the **New** icon highlighted below.

Update Groups

Current Groups

Group

1000
1000*74
1001
1001*74
1020

Group 1000 contains:(1)

First Name	Lastname	Department
1000	Avaya 9641 SIP deskphone	

Enter a **Name** for the new group. From the left window locate the new user added previously and select this by clicking on the right arrow highlighted. Then click **Save** (not shown).

Edit Group

Name of group

Name

☒ Default ☐ On-Call Service ☐ Ad hoc

All recipients

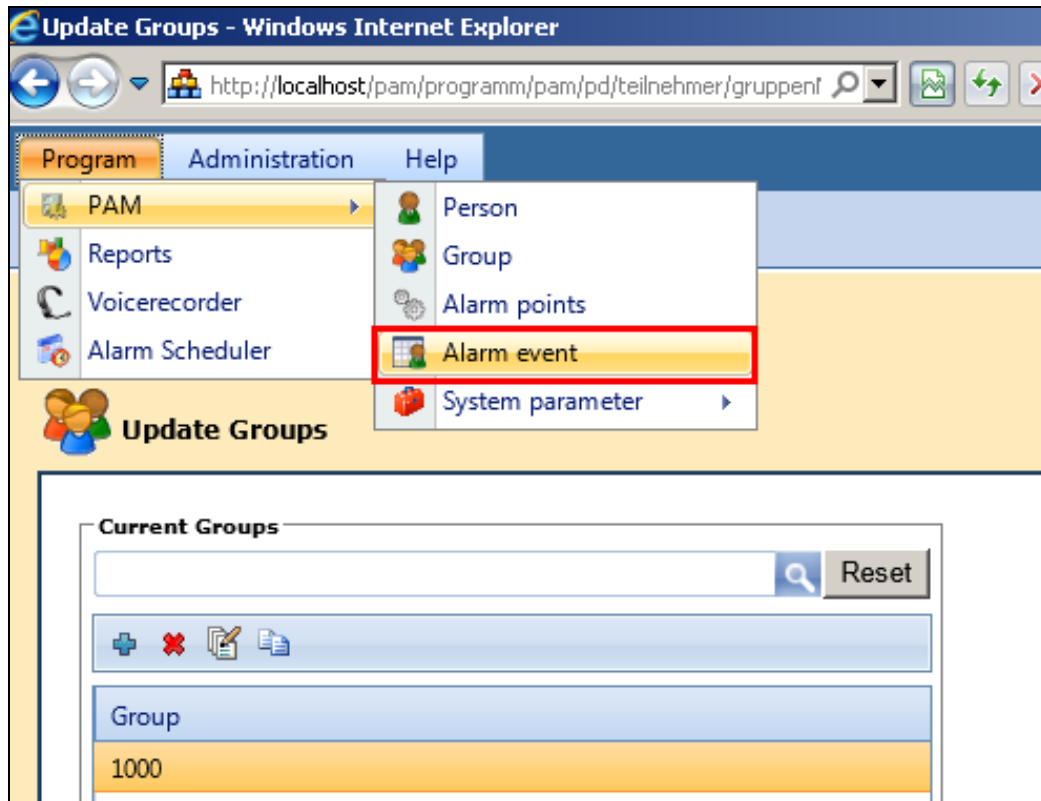
<input type="checkbox"/>	First Name	Lastname	Department	Communication	Target ID
<input type="checkbox"/>	1001	Avaya 9630 SIP deskphone		INT L-15-1	1001
<input type="checkbox"/>	1001	Avaya 9630 SIP deskphone		*74CFD-L-5-1	*741001
<input type="checkbox"/>	1001	Avaya 9630 SIP deskphone		INT L-15-1	22251001
<input type="checkbox"/>	1000	Avaya 9641 SIP deskphone		INT L-15-1	1000
<input type="checkbox"/>	1000	Avaya 9641 SIP deskphone		*74CFD-L-5-1	*741000
<input type="checkbox"/>	1000	Avaya 9641 SIP deskphone		INT L-15-1	22251000
<input type="checkbox"/>	2200	Avaya DECT H.323 handset		INT L-15-1	2200
<input type="checkbox"/>	1020	Avaya Flare (SIP)		*74CFD-L-5-1	*741020
<input type="checkbox"/>	1020	Avaya Flare (SIP)		INT L-15-1	1020
<input type="checkbox"/>	1020	Avaya Flare (SIP)		INT L-15-1	22251020

Group 2200 contains:(1)

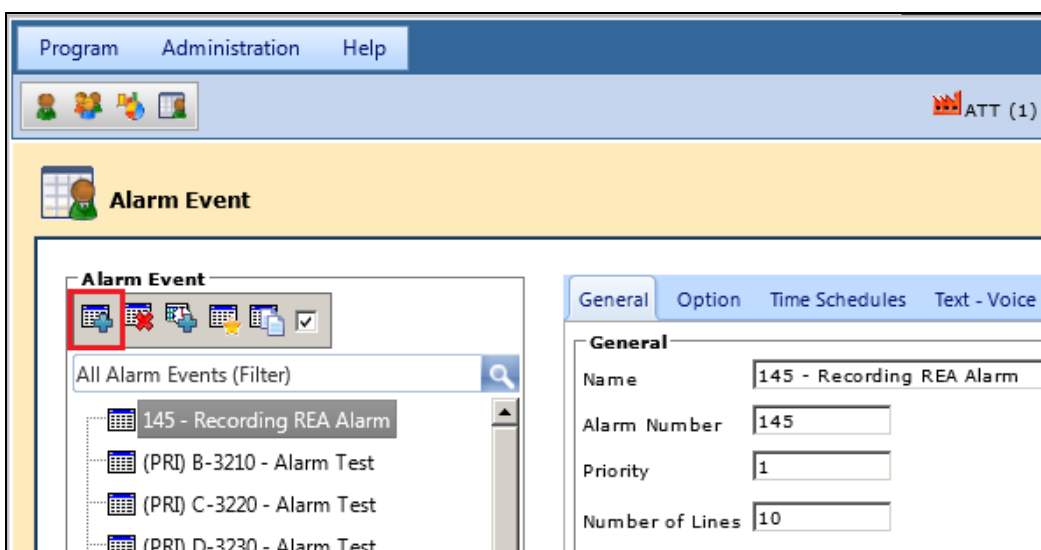
<input type="checkbox"/>	First Name	Lastname	Department
1 <input type="checkbox"/>	2200	Avaya DECT H.323 handset	

7.2.3. Create an Alarm Event

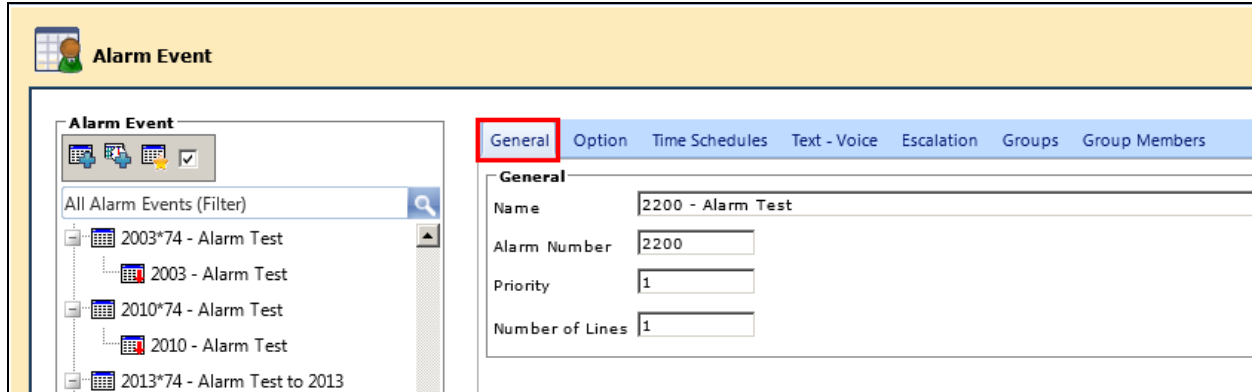
In order to send an alarm, an alarm event must first be created. Select **Program→PAM→Alarm event**.



In the resulting window click on the **New** icon highlighted below.



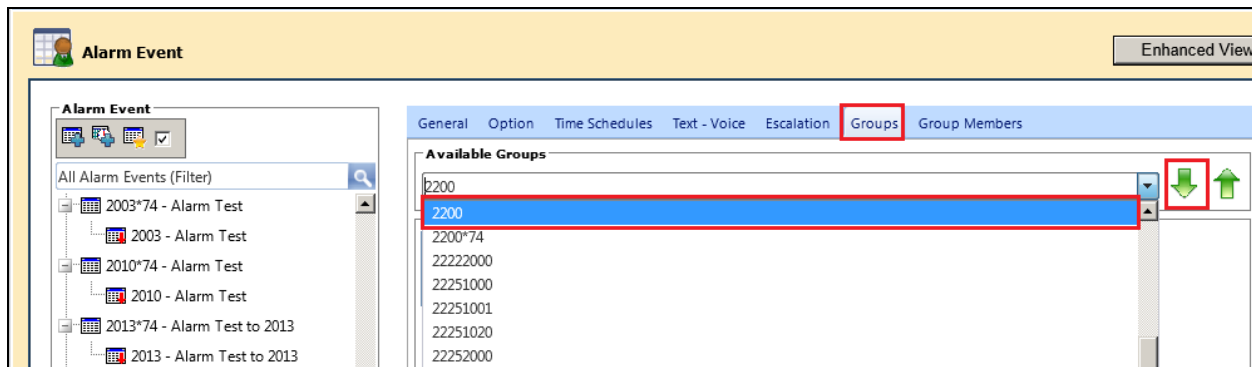
In the **General** tab enter the details of the new event such as the **Name** and the **Alarm Number**.



The screenshot shows the 'Alarm Event' window with the 'General' tab selected. The left sidebar lists various alarm events. The main area contains the following fields:

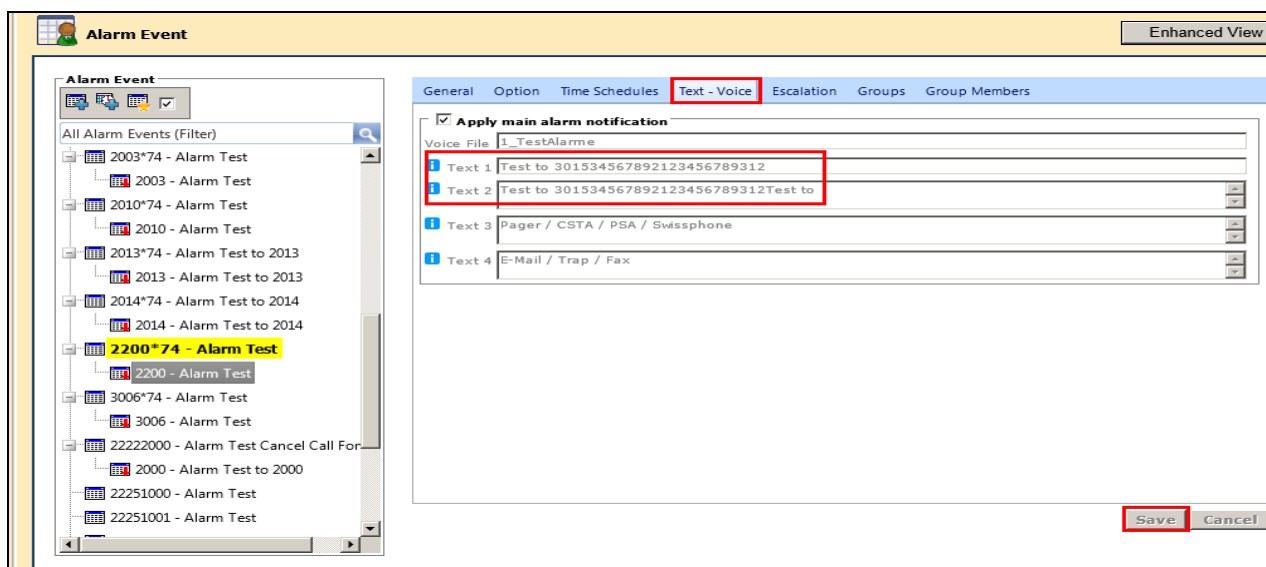
General	
Name	2200 - Alarm Test
Alarm Number	2200
Priority	1
Number of Lines	1

Click on the **Groups** tab and select the group created in the previous section. Click on the down arrow highlighted to add this to the Alarm Event.



The screenshot shows the 'Alarm Event' window with the 'Groups' tab selected. The left sidebar is the same. The main area shows a list of 'Available Groups' with '2200' selected and highlighted in blue. A red box highlights the down arrow icon next to the selected group, indicating it should be added to the event.

All other tabs can be left as default, such as **Text-Voice** shown below which has a certain text associated with it created during the install. Click on **Save** once complete.



The screenshot shows the 'Alarm Event' window with the 'Text - Voice' tab selected. The left sidebar shows the event '2200*74 - Alarm Test' highlighted in yellow. The main area contains the following fields:

Text - Voice	
<input checked="" type="checkbox"/> Apply main alarm notification	
Voice File	1_TestAlarme
Text 1	Test to 301534567892123456789312
Text 2	Test to 301534567892123456789312Test to
Text 3	Pager / CSTA / PSA / Swissphone
Text 4	E-Mail / Trap / Fax

At the bottom right, there are 'Save' and 'Cancel' buttons. The 'Save' button is highlighted with a red box.

8. Verification Steps

The following steps can be taken to ensure that connections between ATT AMX server and Session Manager and Communication Manager are up.

8.1. Show SIP entity is up on Session Manager

Log into System Manager as done previously in **Section 6.1**, select **Session Manager** (not shown). Click on **SIP Entity Monitoring** as highlighted below. Note that the SIP Entity, **10.10.40.80** (ATTAG SIP Entity address), shows **UP** and **200 OK**.

SIP Entity, Entity Link Connection Status

This page displays detailed connection status for all entity links from all Session Manager instances to a single SIP entity.

All Entity Links to SIP Entity: ATTAG

Summary View

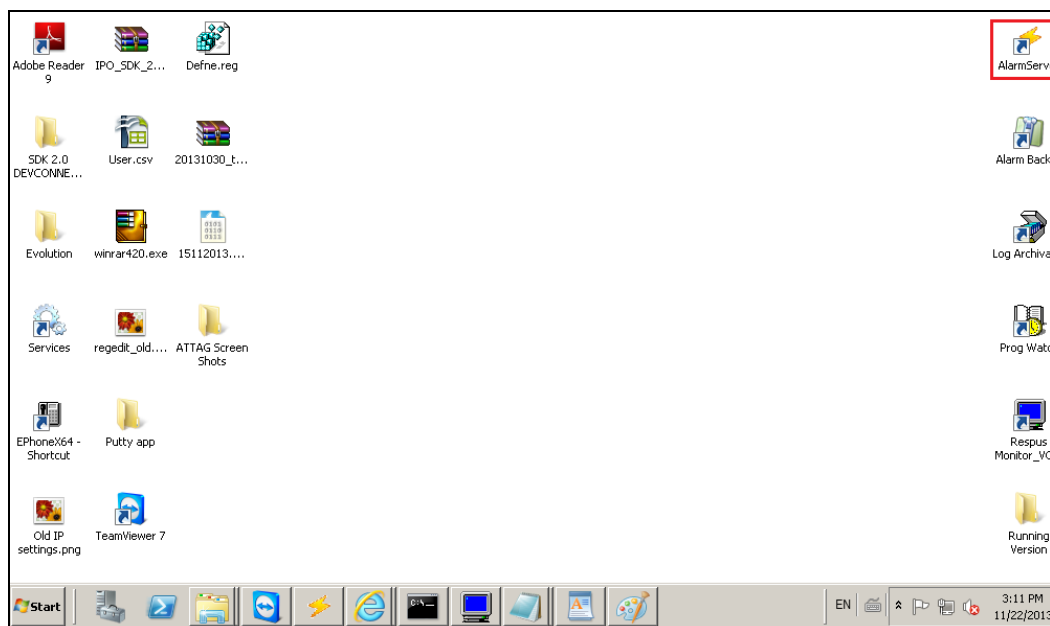
Status Details for the selected Session Manager:

1 Items | Refresh Filter: Enable

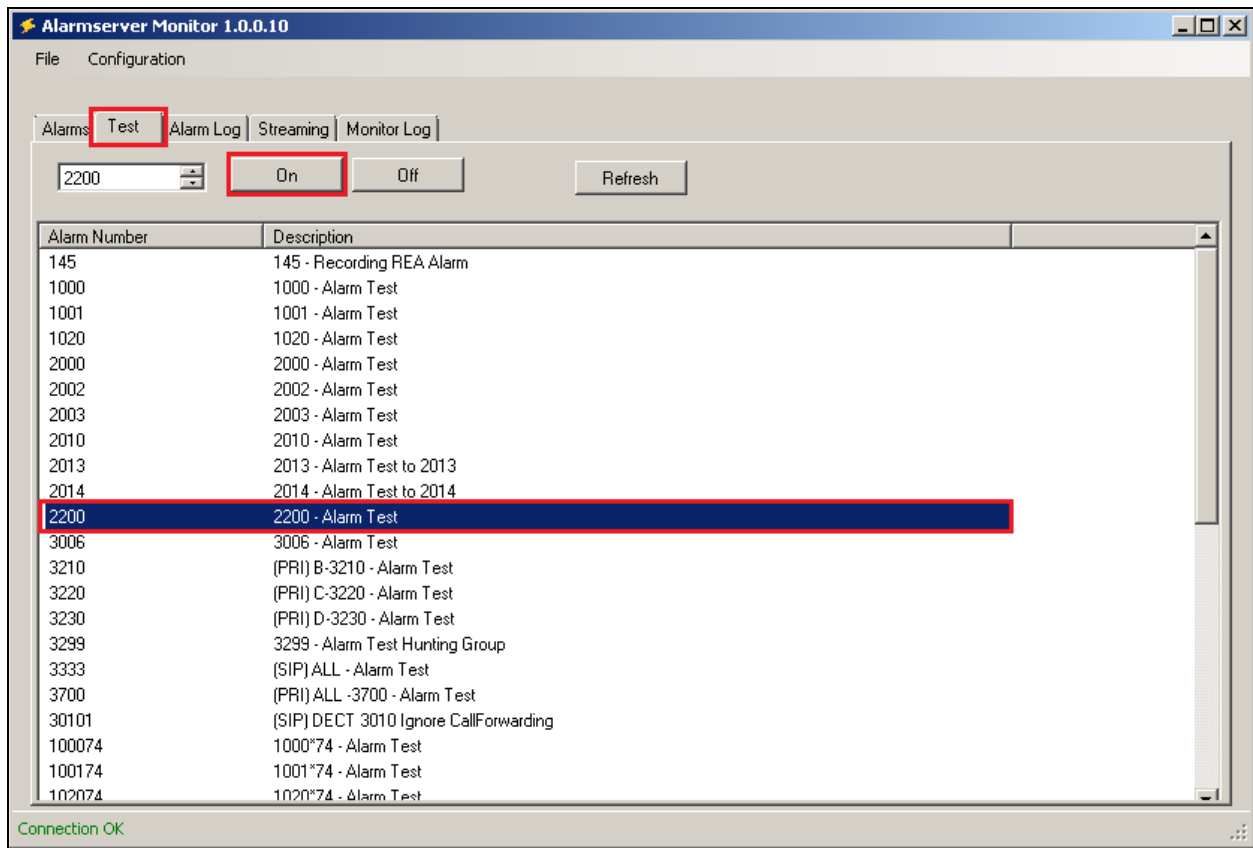
Session Manager Name	SIP Entity Resolved IP	Port	Proto.	Deny	Conn. Status	Reason Code	Link Status
SM63vmpg	10.10.40.80	5060	UDP	FALSE	UP	200 OK	UP

8.2. Show alarm is sent on the AMX Alarm Server

Open the Alarm Server by clicking on the **AlarmServer** icon highlighted on the screen below.



Click on the **Test** tab and select the alarm event created in **Section 6.2.3**. Once selected click on the **On** button highlighted below. The extension associated with the event should ring, allowing the alarm be heard correctly from that extension once answered.



9. Conclusion

These Application Notes describe the configuration steps required for ATT-AudioText Telecom AG Alarm Management Server to successfully interoperate with Avaya Aura® Communication Manager R6.3 and Avaya Aura® Session Manager R6.3 by registering the Alarm with Avaya Aura® Session Manager as third-party SIP user. Please refer to **Section 2.2** for test results and observations.

10. Additional References

This section references documentation relevant to these Application Notes. The Avaya product documentation is available at <http://support.avaya.com> where the following documents can be obtained.

- [1] *Administering Avaya Aura® Communication Manager*, Document ID 03-300509
- [2] *Avaya Aura® Communication Manager Feature Description and Implementation*, Document ID 555-245-205
- [3] *Implementing Avaya Aura® Session Manager* Document ID 03-603473
- [4] *Administering Avaya Aura® Session Manager*, Doc ID 03-603324

Please refer to **Section 2.3** of these Application Notes for information on ATT support.

©2014 Avaya Inc. All Rights Reserved.

Avaya and the Avaya Logo are trademarks of Avaya Inc. All trademarks identified by ® and ™ are registered trademarks or trademarks, respectively, of Avaya Inc. All other trademarks are the property of their respective owners. The information provided in these Application Notes is subject to change without notice. The configurations, technical data, and recommendations provided in these Application Notes are believed to be accurate and dependable, but are presented without express or implied warranty. Users are responsible for their application of any products specified in these Application Notes.

Please e-mail any questions or comments pertaining to these Application Notes along with the full title name and filename, located in the lower right corner, directly to the Avaya DevConnect Program at devconnect@avaya.com.